論文

情報社会における逆機能の問題と対策

── コンピュータ犯罪を中心に ──

洪　承　演

要　旨

コンピュータと情報通信技術による高度情報社会の到来は，社会のあらゆる分野に大きな変化を持ってきて，多くの附加価値の創出と共に多様な便益を順機能として提供している。反面，これに伴うたくさんの逆機能も現れているのも現実である。そのなかで特にコンピュータ関連犯罪による被害が次第に増加している。コンピュータ犯罪とは，このような逆機能の一つとして登場した情報社会の新種犯罪で，情報化が進展すればするほど色々な分野で発生して，その犯罪の様相も次第に深化している実情である。このような状況は，コンピュータ犯罪に関する研究とその制御のための努力がより一層必要な時期ではないかと考えられる。

本稿では，情報社会の明と暗の部分として情報社会に伴う逆機能の中でコンピュータ犯罪に対して，特に日本と韓国の現状を考察しながら，その拡散防止のための管理方案を提示することにする。それによって，コンピュータ犯罪に対しての研究と対策樹立に参考になるように進めようとする。

キーワード：情報化，情報社会，コンピュータ犯罪，逆機能，ハッキング

1．情報社会の明と暗

21世紀を目前にして，世界は確実に歴史的過程としての「情報化」，つまり工業社会から情報社会への文明史的転換の道を辿っている[1)]。ダニエル・ベルが後期産業社会を話した以来，精神産業社会，コミュニケーション等いろいろな概念が登場した。これらのすべてが情報社会の波を描写する概念である[2)]。「情報」という用語は，広義にはニュースや知識を指すのにも用いられているが，厳密には，人間を離れて客観的に伝達・処理ができるようになった段階で

のそれをいう。「情報社会」とは，コンピューターによる迅速な情報処理と，多様な通信メディアによる広範な情報伝達によって，大量の情報が不断に生産，蓄積，伝播されている社会をさす。

通信技術とコンピューターの飛躍的な発達を背景として，1960年代後半ころから日常的にも広く用いられるようになった用語である。物質やエネルギーの変形・処理を主要な産業とする工業社会の後に到来する社会という意味での「脱工業社会（post-industrial society）」と概念的にほぼ同義である[3]。情報社会は「産業の情報化」と「情報の産業化」が同時になされる社会である。産業の情報化とは，情報通信技術が産業の下部構造化する現象をいう。また，情報の産業化とは情報その自らの経済的価値を認めて，情報生産，情報流通産業などが発達する現象をいう。今までの情報化政策は，主に産業の情報化や超高速情報通信網など，物理的な情報基盤施設に対しての投資政策に主眼点をおいてきた。

しかし，情報社会の成熟のためには，情報の産業化と関連した制度の整備と政策の推進も重要だと考えられる。情報化関連法と制度の整備の中で，最も核心的な事項はやはり情報化と共に現れる各種の逆機能を最小化するためのことである。情報化が生み出している逆機能を効果的に制御できないならば，情報化による便益は否定的な逆機能によって相殺されるためである。情報化を促進することができるように関連制度，法，機構などを構築すると同時に，逆機能を予測・分析して，情報化と関連している副作用を最小化しなければならないことである。

情報社会としてのインターネット上に展開されている世界は国境が存在しない。ネットワーク上に登録されるそれぞれの情報は，距離的な概念が存在しないですから，一度インターネット上の世界に入り込んでしまえば，国内・外の情報を瞬間に入手することが可能になることである[4]。今からのインターネット時代，すなわち産業の革命時代は[5]，情報化が国際的な産業構造のレベルの問題になり，さらに産業を超えてあらゆる一般的な社会生活の全盤に浸透する時代になると考えられる。

しかし，情報化が引き起こす逆機能は，非常に多様になっていることが新しい時代の阻害要因である[6]。

本稿には，情報社会が引き起こしているいろんな問題のなかで，逆機能としてのコンピュータ犯罪に関する問題と対策に中心議論をおいて，特に，今後の研究テーマとしての日・韓中央行政機関の公務員のコンピュータ犯罪に対する意識比較調査分析のために，日本と韓国の現状を考察しながら進めようとする。

2．情報社会に現れる逆機能

情報化は順機能と共に逆機能を持ってくる[7]。ある社会活動ないし制度が，その結果において他の社会活動ないし制度の働きを損なうことがある場合，逆機能を果たしているという。どんな個々の活動も他のある活動に対しては逆機能を果たし，また別の活動に対しては促進する機能としての順機能を果たすことである。また，同じひとつの活動に対して逆機能と順機能の混合機能を果たすこともある[8]。

まず，本稿の主題としての逆機能を詳細に検討する前に，情報化の順機能を少し注意深くみようとする。情報化は予見される，あるいは予期できない多くの副作用を産んでいるけれども，情報技術の発展は肯定的な側面でも，人類史の流れを変えて置くほど，その影響は大きい。インターネットを中心とするコンピュータ・ネットワーク時代には，コンピュータが単に特定者の専用ではなくて一般の人も接することになってから，それと一体化しなければならないと思われる[9]。情報化とは情報機器産業はもちろん，情報サービス等の新しい産業が経済規模を拡大させるだけでなく，新しい雇用機会などの附加価値を創出する社会である。また，情報化の波は政治と行政などいろんな分野にも大きな影響をおよぼしている。国家の行政業務も情報化に伴った行政能率の向上によって急速になされている。こなような情報通信革命は大量の情報を速かに処理できる情報技術を画期的に発展させて，それによって人間が享受する生活の質が向上させている。通信とコンピュータを組み合わせて，総合的に「情報」を取り扱うシステムを構成すれば，相乗効果でより有益な特徴を発揮させることができる[10]。そのゆえに，世界の各国が情報高速道路の構築，情報化教育，法体系及び制度の整備など，高度情報社会に進入するために，たくさんの費用を支払っている理由も情報化がもたらす莫大な順機能を念頭に置いたことである。

しかし，小銭の両面のように情報化は順機能と逆機能を共に持ってきている。情報化が引き起こす逆機能は，例えば，行政の情報化に伴う一般国民の私生活侵害の可能性，技術の発達によるコンピュータを利用した各種犯罪の増加，コンピュータ・ウィルスの問題，新しい社会の情報疎外問題などで登場している。また，社会的な問題としてアンダクラス（Under-Class）を産む情報遅滞現象，情報化に対する不適応の原因で来るテクノストレス等も，解決しなければならない逆機能ということで現れる現象である。新しい情報社会の可能性に対して，新しい社会的な問題として著作権の問題，電子マネーの問題，猥褻物の規制問題等，いろんな問題があるが，その中で，一番重要な問題はコンピュータを利用している犯罪の問題である[11]。また，去年の話題は，「西暦2000年問題，ミレニアム・バグ」で，2000年1月1日になってから，コンピュータが使えなくなるようになってしまうということであった[12]。

こうした情報社会の逆機能としての情報化と共に現れる危険性に対して分類しようとする。情報社会はコンピュータ・システムによる情報処理に対しての依存度が高くなって，その依存度はコンピュータ・システムと技術発展の進歩と共にもっと高くなっている。このような情報化と共に現れる危険性を①自然環境の災害と異変，②システム構成装置の故障，③人間の善意行動と過失，④人間の悪意行動と故意の四つのカテゴリーに分類ができる[13]。このような情報化の役割を担っているコンピュータの危険性を自然災害・故障・事故と故障，運用管理上のエラーとか失敗・過失，犯罪に分けて分類することもできる[14]。

高度情報社会には，情報の量が爆発的に増大するから情報の不明瞭性，不確実性ないし不真実性も増大するから，情報における意味の拡散は，現実の曖昧性を増大させ，さらにノイズを氾濫させるのは当然なことである[15]。このような情報化によるコンピュータを利用する各種の犯罪の増加など，情報化に伴う問題点が指摘されていることである[16]。

3．コンピュータ犯罪に対しての考察

犯罪は，罪を犯す行為や，犯した罪自体をいう。狭義では法に規定された違法行為だけをいうが，最広義では罪と同義で反社会的・反権威的行為のすべて

をさしている[17]。また，犯罪とは，社会秩序を侵害する反社会的・反文化的・反規範的行為で，刑罰を科すのが相当であるような行為だと定義している[18]。情報社会で問題になっている犯罪現象の中で，代表的なものがコンピュータによって処理した情報と資料に関連している犯罪で，これらをコンピュータ犯罪（Computer Crime）だと定義している。

コンピュータ犯罪は，広義には，なんらかの形でコンピュータに関連する意図的な非合法行為で，それによって被害者に損失を，加害者に利益をもたらすか，もたらす可能性をもつものをいう。狭義には，その犯行にコンピュータ技術についての知識が不可欠であるような不法行為を指すことである[19]。コンピュータ犯罪は，伝統的な一般犯罪とは違う様相を持っているので，それを犯罪的な側面とコンピュータ犯罪者の動機的な側面に分けて分析すろことができる。まず，動機面としてのコンピュータ犯罪は，ただ自身の知的冒険心を充足するための動機，個人と会社に対する怨恨とか不満をもっている者によってコンピュータを利用した犯行が多く発生している[20]。

また，コンピュータ犯罪者の側面として分析すると，コンピュータに関する特殊技術ないしコンピュータに対する近接が可能になるとき，その犯行が可能になることである。コンピュータ犯罪者は，コンピュータ専門家とかその組織の内部人[21]，罪意識の欠如（伝統的な犯罪とは異なるコンピュータ犯罪には，犯罪意識が希薄であることが一般的な現象です。もっとも重要な理由は行為者と被害者が遠くに離れていることで，行為者と被害者の間には人間ではなくてコンピュータが介入している事実である。行為者が被害者を直接な相手として犯行をすることではないから，犯人の道徳的な抑制力を克服するのは難しいことである。そして，被害者が受ける被害が今すぐには把握されないままの状態で存在することになる。また，行為者の目にも可視的に見えることでもないですからもっと犯罪者の犯罪意識を弱くさせるようになる)[22]，若い年齢層の三つの特異な現象があるのがコンピュータ犯罪と一般犯罪とを区別するべきな特徴だと定義することができる。

また，こうしたコンピュータ犯罪行為が動機的な側面としての社会のアノミー理論と犯罪行為が行為者的な側面としての分化的接触理論の観点から説明することができる。アノミー論とは，アノミー（anomie）の概念を基軸に社会の

病理性とそれに対する人々の適応様式を説明しようとする理論である。デュルケーム（E. Durkheim）によれば，社会規範がその機能の遂行に障害をきたし，その結果，個人の欲求充足行動を適切に（道徳的に）方向づけることができないような社会的無規範状態として定義した。アノミーとは，文化的目標と制度的規範の2つを主要要素とする文化構造の崩壊として定義される[23]。情報通信技術による急激な社会変動の過程に従来の規範が揺れる状態，情報社会に対して新しい規範体系が確立しないことによる規範の混乱または無規範の状態，人間性喪失の状態になってしまう現象をアノミー状態と言うのができる。こんなときは，犯罪に対する罪意識が希薄な状態で，好奇心と英雄心または成就慾が作用することになる可能性が高くなる。即ち，このような情報社会における社会のアミノー現象によるコンピュータ犯罪意識の欠如のせいで新しい規範が確立されなかったのがコンピュータ犯罪を発生させる重要な原因である。

また，犯罪行為の行為者側面から考察すると，サザランド（E. H. Sutherland）の「分化的接触理論（differential association theory）」で説明することができる。サザランドは，犯罪原因について犯罪行動を学習されるし，人々は犯罪的な文化と接触などの9つの命題によって犯罪的文化に同化することをミード（G. H. Mead）の象徴的相互作用理論の影響を受けて定義した[24]。犯罪集団ないし犯罪の誘惑に弱い個人との相互作用（接触）を通じて犯罪行為を学んだりまたは犯罪を行為することになるのがその見解である。犯罪行動は他の非犯罪的な行動と同じく他の人々との相互作用の中で学習されるものであり，人は犯罪的な行動様式と接触し，非犯罪的な行動様式から隔絶されているから犯罪者となるというものである。この分化的接触理論を修正するものとして，人は自己の犯罪行動を受容してくれるだろうと思われる実在または架空の人に対する自己同一化の程度によって犯罪を行うようになるというグレイザー（D. Glaser）の「分化的同一化論（differential identification theory）」や，自分自身についてのよいイメージが非行抑制の重要な要素であるとするレックリス（W. C. Reckless）の「自己概念論（theory of self-concept）」などの理論がある[25]。コンピュータ犯罪は大体にコンピュータに対して専門的知識がある者によって行われている[26]。こうしたコンピュータに関する専門人によって行われるコンピュータ犯罪こそ，分化的接触理論によってその原因として説明するの

ができると思います。

そして，コンピュータ犯罪自体の概念を否定説と肯定説から検討すると，否認すべきだという否定説は，コンピュータ自体は犯罪的ではないですから概念自体が不正確なものだけではなくて，不明確な事件等の単純な集合体だということである。肯定説は，広義的な概念と狭義的な概念，最狭義的な概念に区分できる[27]。コンピュータと関連した反社会的な行為または[28]，資料の自動処理及び伝達を包含している不法的，非倫理的，無権限的な行為等がコンピュータ犯罪ということが広義的な概念である。コンピュータ資料と関連付けて発生している財産的な侵害行為を惹起する，故意がある犯罪行為の総体がコンピュータ犯罪ということは狭義的な概念である[29]。狭義のコンピュータ犯罪の中で，現金引き出しカードと各種のクレジット・カードを利用する犯罪だけをコンピュータ犯罪と分類しようというのが最狭義的な概念である[30]。

このように，コンピュータ犯罪の概念は多様に提示されているが，大きく広義の概念と狭義の概念に分けて見ることで，大部分の学者はコンピュータ犯罪を広義で解析している。日本警視庁は，コンピュータ犯罪を「コンピュータ・システムに加えられる犯罪ないしこれを悪用する犯罪の総体」と規定して広義的な見解を見せている[31]。米国政府は，「コンピュータ関連犯罪」という用語を使用しながら，コンピュータ犯罪を，広義的に解析して「コンピュータ犯罪はコンピュータ・プログラムを操作することと同じで，きわめて技術的に洗練された犯罪はもちろん，コンピュータ・システムに対する虚偽入力と出力の誤用で由来すること」という定義をしている。したがって，コンピューター犯罪は「コンピュータが行為の手段または目的とするあらゆる犯罪行為」を指し示すことが広義的な概念である。

反面，狭義的な概念は，コンピュータ犯罪をコンピュータ資料と関連して発生する財産的な侵害行為を惹起させる故意の犯罪行為の総体だと定義する見解である[32]。したがって，狭義的な概念はコンピュータ犯罪の概念の中で，財産以外の法益に対する侵害は除外する。情報社会が進展することによって，既存の財産権に対する概念を脱皮した技術，情報など新しい形態の財産権の概念が胎動する現実を勘案すれば，コンピュータ犯罪の概念は広義的に解析することが妥当だと考える。

最近，情報社会の発展と共に，高速なコンピュータ通信技術によって国際的なインターネットを通したネットワークを利用するコンピュータ犯罪が頻発している。特に，インターネットにおいては，誰かがどこから使っているかがわからないため，専用ネットワーク以上にコンピュータ犯罪に対しての注意が必要とする[33]。また，ネットワーク犯罪とは「コンピュータや周辺機器を利用して，一つまたはその以上のコンピュータが，有・無線で連結した特定な通信網内の特定コンピュータに非正常的な方法で接続したり，正常な方法で接続した後，不正の意図がある一切の行為及びネットワーク文化を混乱させる一連の行為」だと定義する[34]。もちろん，ネットワーク犯罪も広義のコンピュータ犯罪の範疇に属することだが，超高速情報通信網の構築とか各種の電算網構築で，広域化になっている現実を勘案すれば，今後もこのような類型の犯罪がより一層頻発することと見られる。しかし，本稿にはネットワーク犯罪をコンピュータ犯罪でその用語を使用するようこととする。

このようなコンピュータ犯罪の基本的な概念は，1997年６月に開催されたＯＥＣＤデンヴァー・サミットの「コミュニケ」で，「コンピュータ技術及び電気通信技術を悪用した犯罪」を意味する言葉として用いられており，その後から国際的に定着した用語となっている。これは，刑法に規定されている電子計算機損壊などの業務妨害罪をはじめとしたコンピュータもしくは電磁的記録を対象にする犯罪またはそれ以外のコンピュータ・ネットワークをその手段として利用する犯罪である。犯罪ということができるこのようなコンピュータ犯罪の概念は[35]，ＯＥＣＤの定義によると，「自動的データ処理システムまたはデータ通信システムを考慮に入れて実行される，法律違反，または倫理的なもので，あるいは許容されないすべての行為態様として特徴づけられるもの」と定義している[36]。

コンピュータ犯罪に対しての日本の関連機関の定義は次のようになります[37]。通産省は，コンピュータが直接的あるいは間接的に何らかの形で介在した社会悪行為で，警察庁は，情報システムに関わる犯罪を「ハイテク犯罪」として総称しながら，コンピュータ犯罪とは，コンピュータ・システムの機能を阻害し，またはこれを不正に使用する過失を含む犯罪として，またネットワーク犯罪とは，コンピュータ・ネットワークを手段として用いる犯罪としてコンピュータ

犯罪以外のものと定義している。また，ＯＥＣＤは，コンピュータ犯罪をコンピュータおよび電気通信技術に対して，国境を越えて介入するような犯罪だと定義している[38]。

このようなコンピュータ犯罪を行なう犯罪者の呼び方[39]について次のように区分することがでる。まず，クラッカ（破壊者）とはコンピュータ・ウィルスを流布してコンピュータを混乱させたり，故意にコンピュータに障害を引き起こさせる犯罪者をいう。その目的は愉快犯，あるいは怨恨などによる行われると言われている。また，アタッカ（侵入者，攻撃者）とは，コンピュータへの不正侵入やネットワーク上を流れるデータを盗聴することによって，データを不正に盗み出したり，改竄，悪用する犯罪者という。その目的は愉快犯的なことから盗み出したデータを悪用することである。

次には，コンピュータとネットワークと関連付けてコンピューター犯罪の類型を分析すると，大きく分けてコンピュータ不正操作，コンピュータ破壊，コンピュータ・スパイ，コンピュータ無権限使用[40]，コンピュータ通信上の不正行為など非常に多様に現れている。犯罪類型は，コンピュータ技術が発達すればするほど新しい類型の犯罪がずっと派生するものと見られる[41]。このようなコンピュータ犯罪の行為的類型には，コンピュータ・ウィルスの製作と流布，ハッキング・クラッキング，金融犯罪・電子詐欺，猥褻サイトーの運営，サイバーテロ，マネーロンダリング，偽情報による嫌がらせ，電子ストーカー，盗聴・漏洩，情報の改竄，成りすまし，事後否認，不正行為に関する情報の発信，暗号の不正利用などがある。猥褻サイトーに対して日本の場合は伝統的な規制だが，米国では「猥褻」と「下品」の二種類の概念で区別している[42]。

コンピュータ犯罪に対しての日本の関連機関の類型を考察すると，通算省は，金銭の不法領得，コンピュータ・システム及びデータ等の破壊，マシンタイムの盗用，コンピュータ関連資産の窃取等で区分している[43]。警察庁は，コンピュータまたは付帯設備の損壊，磁気テープ・磁気ディスクまたは光ディスクなどの損壊，コンピュータの機能を阻害するためのデータ又はプログラムの改竄，ハードウェアの不正使用，データまたはプログラムの不正入手，システムを不正に使用するためのデータまたはプログラムの改竄等で区分している。また，ＯＥＣＤは財産利得罪，偽造罪，機能妨害罪，プログラム著作権の侵害，不正アク

セス等でコンピュータ犯罪の類型を分類している。一方において，コンピュータに基づくデータの収集，貯蔵，結合及び転送によって国民のプライバシーを脅かすこともコンピュータ犯罪の範疇に含めている。コンピュータ・システムおよびネットワークに対する攻撃やこれらを用いた犯罪であり，成立用件にコンピュータの存在が必要である犯罪として定義している[44]。

こうした複雑し多様な類型のコンピュータ犯罪の行為を一定的な基準によって分類しようとしましたけど，現在までにはその分類方法が一定的に定めているではないが，【表１】[45]のように学者によってその類型が分類される[46]。

こういうコンピュータ犯罪の特徴には，一般の犯罪とは異質の面が多いので，次のように区分することができる[47]。１）摘発と原因糾明の困難性，２）犯行の国際性と広域性，３）犯罪の痕跡の困難性，４）犯罪意識の稀薄化，５）犯行の自動性と反復性および連続性，６）専門家または経営内部者の犯行が多いことである。

また，コンピュータ犯罪の特徴に対しての分類は次のように分類することもできる[48]。１）匿名性が高い，２）犯罪の痕跡が残りにくい，３）不特定多数の者に被害が及ぶ，４）暗号による証拠の隠蔽が容易，５）国境を越えることが容易であることである。インターネットはグローバルなコンピュータ・ネットワークを利用して，国境を越えた情報の伝達・交換を瞬時に行うことができるため，コンピュータ犯罪は，従来の人，物，金の移動を伴う犯罪に比べてその国際的性格が顕著である[49]。

また，コンピュータ犯罪は，発見の困難性，犯人特定の困難性，成功率の高いこと，内部犯行における長期間の継続性，有効な対策が存在しない，法的には国境も法律もない[50]，社会的影響が大きい，犯罪の物理的な証跡が残らず無痕跡性，被害金額の大きいこと，被害の無届けに区分して分類することもできる[51]。

こうしたコンピュータ犯罪は，コンピュータに対しての基礎ないし専門知識が必要とするので，専門家または内部者等によって犯される場合が多いことである。

【表１】学者によるコンピュータ犯罪の類型分類

学　者　名	コンピュータ犯罪類型
1）Louis Rohner	①　操作 ②　コンピュータ不正使用 ③　スパイ ④　破壊
2）Klaus Tiedemann	①　操作：損害の範囲と行為の方法を基準に ②　産業スパイ：電子資料の処理領域で ③　破壊：電子資料の処理領域で ④　不正使用
3）Ulrich Sieber	①　資料変更 ②　資料の無効化 ③　不法的な資料の獲得と資料の利用 ④　コンピュータ・ハードウェアに対する攻撃
4）August Bequai	①　破壊 ②　用役窃盗 ③　財産犯罪 ④　資料犯罪
5）Donn B. Parker	①　破壊による損害 ②　情報とか財産の詐欺または窃盗による損害 ③　財政的な詐欺または窃盗による損害 ④　無権限使用および用役販売による損害
6）Wolfgang Steinke	①　コンピュータ詐欺 ②　コンピュータ・スパイ ③　コンピュータ破壊 ④　コンピュータ盗用
7）倉　橋　　宏	①　コンピュータを悪用する行為 ②　コンピュータを損害する行為 ③　コンピュータによって得る情報を漏洩または窃取して使用・悪用する行為
8）門　田　　渉	①　ＣＤ犯罪 ②　不正データの入力 ③　データ，プログラムなどの不正入手 ④　コンピュータ破壊 ⑤　コンピュータ不正使用 ⑥　プログラムの変更・消去 ⑦　磁気データ等電磁的な記録物の損壊
9）的　場　純　男	①　データの不正操作 ②　データの不正入手 ③　コンピュータの無権限使用 ④　コンピュータの破壊

4．コンピュータ犯罪の問題

4－1．コンピュータ犯罪の暗数問題

暗数（Dark Figure）とは，現実に発生しているであろう犯罪の数と警察の認知件数との差をいうことである。警察が不法事犯の存在を知ったが，軽微性や行政処分の有効性を考えて，犯罪として認知せずに処理することも暗数の生じるひとつの理由であるが，主としては市民の側が被害軽微，犯人等との係わり合いへの恐怖，警察への不信等の理由により通報しないことが原因であることである[52]。この観点からみると，コンピュータ犯罪において暗数とは発見にならないコンピュータ犯罪を言うことができる。本来，この用語は犯罪学者らが報道にならない犯罪を言及するために使用した用語である。

コンピュータ犯罪の暗数問題は，次のようにいろんな要素に基礎されている。まず，精巧な科学技術，即ちコンピュータの機能として巨大に圧縮する貯蔵能力と速度は，コンピュータ犯罪を捜し出すのにたいそう難しくなる。また，被害者等が対処する方法に関して不知なことである。多くの被害者は，コンピュータ犯罪の事件に対して緊急に対処する計画を持っていないし，はなはだしくは，コンピュータを使用する時に，どんな安全上の問題があるかに対しても知らないことである。また，被害者等が報道事実に対して不願している問題もあります。

専門家らはこのような暗数要素が，コンピュータ犯罪の発見と摘発に重要な影響を及ぼしていると主張していて，結局コンピュータ犯罪は，発生になったことの中で一部だけに対して，法の執行当局の関心を持つようになって，正確な実際上の損失と犯罪数字を測定するのが難しい実情だと考える[53]。

4－2．コンピュータ犯罪の深化

1990年代の初めまでのコンピュータ犯罪の大部分は，銀行ないし金融機関の端末機を通して，資料を操作したり不正入力することが主流を成し遂げたが，その以後から，コンピュータ普及の拡散，パソコン通信及びインターネット利用の急増と共にコンピュータ犯罪にも，知能化，悪性化，テロ化，そして武器

化等になるような犯罪現象が次第に深化している傾向を見せている。

このように高度情報化した現代社会に行なっているインターネットを新しい通信手段として用いるコンピュータ犯罪者は，その大部分が大学の学生や10代の若者，企業内部の社員，競合者，コンピュータ会社の秘密組織のハッカーやクラッカー，麻薬やマフィア組織からの古いタイプの犯罪者，プロのハッカー，産業スパイのエージェントなどのようにその領域が広がっている[54]。

また，社会が高度に情報化されればされるほど，特定の国家や企業とは相関なしに国境を越えて，新しい情報社会の問題として大きく拡散になることに見える。

4－3．コンピュータ犯罪者としてのハッカーの問題

現在のインターネットやネトワークの発達と共に，ネットワークとかシステムに対する侵入者の脅威と被害を受けた場合の深刻さは大きいが，大多数の企業と機関はこの脅威にまだ感じていないように見える[55]。ハッカーとは，単に，必要としたことが与えられた環境だけを使用する一般使用者とは違って，あふれる知的欲求で自身がコンピュータ・システムに対する操作が可能な限りの全てのものを探して作ってみる人々を意味する。本来，複雑なコンピュータ問題を趣味として解く人を意味したが，次第に他人のパスワードを盗用して公共機関とか組織のコンピュータ・システムに侵入して，コンピュータ資源を無断に複製したり，障害を起こすことを専門的にする人を意味することに変化している。コンピュータがこれだけ身近になると，それを悪用もしくは意図的に犯罪の手段として利用するハッキングが生じることである[56]。

ハッキングという単語の意味は，悪い意味ではなくて，コンピュータ・システムを研究する悪意的な被害を及ぼされない人を示す言葉だったが，この頃は意味が変化になって故意にシステムに被害を与えること，すなわち，クラキングの意味で使われている[57]。ハッカーは情報を盗む一般的なハッカーと資料を削除したり取り出した情報を利用して金銭的な利益を取るなどの行為を行なうクラッカーに分れる。けれども，この頃は二つの区分がなしに，ハッカーという用語で使われるようになりました。ハッカーは，本質的には自身の業績とか才能を表現するためのハッキングするだけの意味，すなわちコンピュータ犯罪

を行なう意味としてのハッキングはしなかった。しかし，これらの行動の動機が好奇心とかいたずら，そして成就欲であっても，このように開発されたいろんなハッキング方法も，時にはコンピュータ犯罪の目的に使われて，競争関係になっている会社内部にある営業秘密の窃取またはシステム内部にあるファイルの内容を修正して，横領の手段に使われることもある。このような理由で，ハッカーの犯罪的な行為は情報社会の中において，阻害の要因として認識されている。特に，ハッカーが国際的な通信網としてのインタネットを通じて，各国の情報システムに接近が可能ようになっていることから，国家的な情報管理体系を立てるべきなことである。また，ハッカーに対する正確な診断を通じて問題を把握しながら対策を準備するのが必要なことである。

このようなハッカーのハッキング技法に対して考察しようとする。使用する資格がない外部人が使用者の名と暗号を利用して，電話線等を通じてコンピュータに侵入した後，自身の目的によって資料を取り出したりシステムに害を及ぼすハッカーは，自身の目標を達成するために，まず目標システムに接続する電話番号と使用者番号を入手した後，暗号を解析するので，この過程を普通ハッキングという。ハッカーのハッキング技法を4種類に分けて注意深くみると次のようになります。1）トロイの木馬の方法がある。2）低次元のハッキング技法で，無数な試みによって暗号を捜し出す方法がある。3）システムに登録を少しの間保留して，正式使用者が自身の暗号を使用する時，暗号を通信上で奪って正式使用者の名と暗号を知る方法がある。4）物理的またはデータ上の資料カスを収集する方法などがある。

このようなハッキングは1994年を起点に発生件数が増えている。もちろん，色々な国でもハッカーによる犯罪が次第に増加していることと見える。今まで，このようなハッカーのハッキングの類型は，主に通信サービスの不法な使用と通信網を通したシステムに無断接続した場合が大部分である。特に，通信網サービス機関としての情報通信会社も，より確実な情報保安の管理が要求されると考えられる。学校や公共機関などでのハッキング問題がたくさん発生していて，システムと機関自体の固有な資料が破損される場合には，その復旧も難しいことになるから，国家的な被害が深刻化するはずである。

5．コンピュータ犯罪の現況

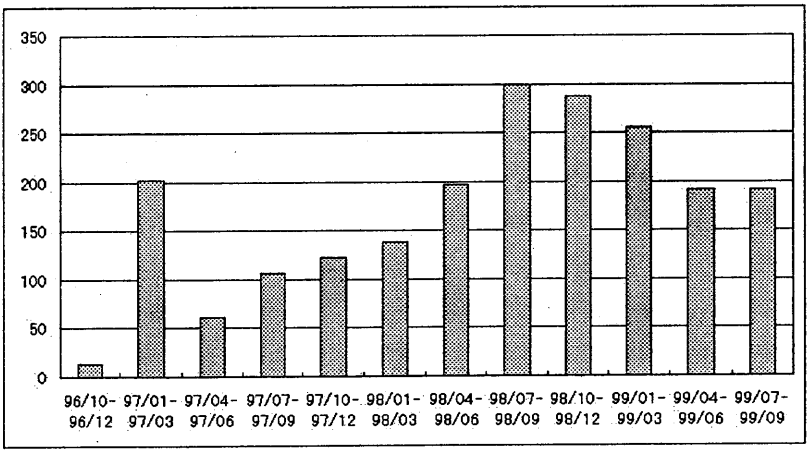
5－1．日本の現況

日本のコンピュータ犯罪の現況に関して，警察庁の最近の主な検挙事例を見ると次のようなことである[58]。1）インターネットを悪用した通信販売の詐欺事件[59]，2）インターネットを悪用したパソコン機器などの通信販売の詐欺事件[60]，3）インターネットを悪用した国際ネズミ講「ペンタゴノ」に係る無限連鎖講防止法違反事件[61]，4）インターネットを悪用した海外の高額懸賞金付ポスト・カード発売の詐欺事件[62]などの最近のコンピュータ犯罪の事例がある。

これらコンピュータ犯罪に対して詐欺事件，無限連鎖講事件，出資法違反事件ごとに区別して，ネットワーク利用の悪質商法事犯に対する日本警察庁の検挙状況をみると1996年の認知件数が8件で，1997年には6件，1998年には12件の現状である[63]。もちろん最近の検挙件数が増えていることが見られることです。

また，JPCERT／CC（日本コンピュータ緊急対応センター）[64]が1996年10月以降に受け付けた不正アクセス報告件数の推移に関して，3ヶ月毎にまとめて，【表2】のようなグラフに現れたことである[65]。

【表2】 不正アクセス報告件数の推移（1999．10．27日現在）　（単位：件）



この表に現れた件数は，JPCERT／CCが受け付けた報告の件数であり，実際の不正アクセスの発生件数を類推できるような数値ではありませんが，1997年度からその数が増えていることがわかる。また，JPCERT／CCの不正アクセスの動向によると[66]，情報提供を受けた不正アクセスの件数は191件で，これらに関して情報提供や情報交換を行ったサイトの数は延べ203サイトでした。

そして，ネットワークに係る犯罪及び不正行為の現象と情報セキュリティ上の課題に対しての現象に対して，日本警察庁が発表した近年のネットワーク利用犯罪等の推移に関して，コンピュータ犯罪を電磁的記録不正作出・詐欺事件，電子計算機損壊等業務妨害（容疑）事件，電子計算機使用詐欺事件，不正作出私電磁的記録供用事件，不正作出私電磁的記録供用事件，業務上横領事件，その他に区分しながら発表したことがある。その全体的なコンピュータ犯罪件数は，1995年の認知件数は8件，1996年には10件，1997年には18件でだんだん増えていることがわかる[67]。コンピュータ犯罪に関して，コンピュータ・システムの機能を阻害し，又はこれを不正に利用する犯罪を言うことである。また，ネットワーク利用犯罪に関して，わいせつ物流布等事件，詐欺事件，著作権法違反事件，薬物販売等事件，名誉毀損事件，その他に区分しながら発表したことには，1995年の認知件数は25件，1996年には79件，1997年には83件でだんだん増えていることがわかる。コンピュータ・ネットワークをその手段として用いる犯罪で，コンピュータ犯罪以外のものをいうのである。また，コンピュータ犯罪[68]に対しての，日本の警察庁の情勢は次のようなことである[69]。ハイテク犯罪とは，「コンピュータ技術及び電気通信技術を悪用した犯罪」を意味する言葉として用いられており，具体的には，コンピュータやデータを対象とした犯罪やインターネットなどをその手段として利用する犯罪等が含まれている。ハイテク犯罪の検挙件数は，1993年には32件，1994年には63件，1995年には110件，1996年には176件，1997年には262件，1998年には415件で，1998年度には前年比58％増加しています。また，1993年と比べると13倍増加しています[70]。

このようなコンピュータ・ネットワークに重大な脅威を与えるコンピュータ犯罪としての不正行為は，高度情報通信社会の健全な発展を阻害する恐れがあるから，早急な対策が必要です。警察庁では，1998年６月に公表した「ハイテク犯罪対策重点推進プログラム」に基づき，ハイテク犯罪対策を進めていくた

めの体制や法制の整備などに取り組んでいます。

5－2．韓国の現況

韓国の場合にも，情報化の急速な進展によってインターネット空間内で，①先端情報通信機術を利用した電算網に対する侵害行為，②ウィルス流布行為等各種新種犯罪が頻発していて，③名誉毀損，淫ら物配布等インターネットを利用した犯罪事件も急増している趨勢にあって，情報化による逆機能による深刻性が次第に現実化している。

韓国における1995年から1999年までのコンピューター犯罪事件は，総350件657人でそのうち180人を拘束したことである[71]。警察庁の新種コンピュータ犯罪の発生現況には，次のように最近の偽造・変造技術と機器の発達によって，クレジットカード及び通化・有価証券などの偽造・変造犯罪が大きく増加していることが現れている。それをクレジットカード関連犯罪，通化・有価証券の偽・変造，知的財産権関連犯罪に分けて【表3】[72]のよに現れている。また新種コンピュータ犯罪の増加が次第に増えていることがわかるようになる。

【表3】 新種犯罪発生現況

（単位：件）

区　　分	1995年	1996年	1997年	1998年
計	9,618	11,762	11,667	13,199
クレジットカード関連犯罪	1,427	1,599	1,691	1,888
通化・有価証券の偽・変造	1,561	1,561	3,349	1,831
知的財産権関連犯罪	6,630	8,339	7,938	8,940

このように増えているコンピュータ犯罪に対して，警察庁はその主要推進事項を次のように推進している。警察庁の知能課にコンピューター犯罪捜査隊を新設（1997．8．4日），コンピュータ関連犯罪等に対して，先端新種犯罪の重点研究指導及び取り締まりなどの主な業務を担っている。また，警察捜査保安研修所にコンピュータ犯罪捜査の教育過程の新設および地方庁及び大都市の警察署の捜査専担178人を教育・配置して活用するようにしている。そして，全国225個の警察署にコンピュータ関連の犯罪捜査機器を設置して，諜報収集及び捜査活動の強化を進めている。また，先端・新種犯罪及び知能犯に対して，

犯罪趨勢を分析するために企画捜査を実施した。その結果，クレジットカード関連犯の取り締まり[73]，不法的な盗聴行為等の関連犯の取り締まり[74]の実績がありました。

このように，コンピュータ犯罪のための専門組織としての「コンピューター犯罪捜査隊」は，コンピュータとインターネットの普及拡散及び商用化，コンピュータを対象としたりコンピュータを利用した新種犯罪の増加，ハッキング等の犯罪手法の先端化及び被害の大型化，回復不可能な傾向，情報化時代の情報戦争としての核心的な手段であるハッキング，コンピュータ・ウイルス技術及び電子商取り引きなどに現れる逆機能に積極的に対応する必要性が増大して創設・活動している。コンピューター 犯罪捜査隊が対象としている犯罪は，ハッキング，ウイルス流布等の専門的で技術的な犯罪，猥褻サイト（ポルノ・サイト）の運営，インターネットを利用した不法行為，パソコン通信を利用した淫ら物，不法複製物等の配布行為，電子商取り引き等の情報化時代の新技術と関連犯罪などである。その活動に対しては，コンピュータ通信網に対する24時間の検索，分析及び捜査体制を維持しながら，専門的で技術的な事件に対てはコンピューター犯罪捜査隊が直接担当している。一般のコンピュータ関連事件に対しては，地方警察庁の専担要員（総251人）によって捜査するようにしている。また，国内・外の専門機関へ委託教育，コンピューター犯罪捜査過程による専門教育を実施しながら，コンピュータ犯罪に対する捜査技法及び人材の養成等を進めている。

また，韓国情報保護センターが調べたコンピュータ犯罪と関連しているハッキングの実態に関して【表４】のように現れている。ハッキング被害の件数が持続的に増加していて，1999年の上半期に既に，1998年の１年間に発生した総件数より多くのハッキングが発生したのが現れている。これを大学，企業，政府機関，非営利機関，研究所，地域，その他に区分して分類してみると，コンピュータ犯罪の対象は大学と企業が多くて，次第に増えていることが現れている[75]。

最近，増えているコンピュータ犯罪とは，情報システムの誤用・乱用的な事例の分類とか発生件数の集計は，分類基準の設定によってその結果が異なる。まだ，統一的な基準がないため，ほとんどの学者とか機関の研究目的によって

【表４】機関別ハッキング被害件数　（単位：件数）

区　分	1996年	1997年	1998年	1999年	計
大　学	95	32	80	100	307
企　業	46	25	69	80	220
政府機関		1	1	1	3
非営利機関	2	1	2	3	8
研究所		3	4	1	8
地　域			2		2
その他	4	2		8	14
計	147	64	158	193	562

その基準を定めて，いろんな形態の分類と集計を行なっている実情である[76]。

6．コンピュータ犯罪に対しての対策

コンピュータ犯罪の対策は，事前予防的な次元で安全対策を樹立するべきで，事後規制的な方法として法的及び刑事政策的な対策が講じるべきなことである。こうした一般的な対策には，技術的には使用者の認識または確認，アクセス・コントロール，暗号化，モニタリンク，通信システムのセキュリティなどがある[77]。このようなコンピュータ犯罪として増加してきた不正アクセスに対処するため，日本の通産省は1996年８月，「コンピュータ不正アクセス対策基準」を告示した[78]。このようなコンピュータ犯罪の対策は，現実の認識と共に次のような基本的な方向が前提されることで，効果的な対策が樹立になることで考えられるその基本的な方向は，綜合的・持続的・社会全体的な対策の樹立が必要，コンピュータ犯罪の対策に対するマインドの拡散と共感帯の形成と教育が必要なことで，そのなかでコンピュータ及び情報化に対する倫理教育強化に対する検討するようにします。伝統的なメディアに対しては，学校とか家庭でも多くの教育機会を持つようになる。しかし，新しい情報通信サービスの場合には，このような教育の機会がそれほどないことである。通信を使用したビジネス分野においては，事業者間の倫理が要求されます。新しいマルチメディア機

器が広く使われるにことによって，電子メールによる情報の交換にもマナーが重要になっている。このような点で，高度情報社会に相応する情報通信の倫理やマナーを開発して，これが学校及び社会教育などを通じて定着になるようなことが必要である。コンピューター犯罪は，予防が最も重要だという点でコンピュータ関連倫理教育は非常に至急で重要な問題である。コンピュータ・ウィルスの拡散などの情報犯罪の場合にも，行為者が犯罪を行っているとの意識が稀薄なまま，自分の技術を誇って，ゲームを楽しむという意識が強いという点で，法的・技術的な対応にも劣らないくらいの情報倫理の定立が必要である。なお一層，情報社会に相応する「人間と技術」に関する倫理観の定立も必要とする。情報産業にあっても，経済価値[79]は，人性価値[80]の情報倫理と同時に創造にならなければならない。人性価値が無視される経済価値は，生活の質を威嚇するようになるためである。

このような点から次には，コンピュータ犯罪の安全対策の類型に関して考察すると，1）技術的な安全対策，2）物理的な安全対策，3）人的な安全対策，4）法的な安全対策などが必要なことです。このような認識から情報社会におけるコンピュータ犯罪に対しての対策としての改善方案を，制度的な側面と情報倫理の確立の側面から考察するようにしようとする。

1）制度的で組識的な側面での改善方案に対して考察するのができる。システムの安全性は，秘密性，無欠性と可溶性の3つを維持することがその主な要素である。それならば，システムの安全性を確保して維持，対策などを計画して遂行することができるべきなことである。同時に，コンピュータ犯罪を改善・保安させて行く専担組織が必要とする。このようなコンピュータ犯罪に本格的に対処するために，発生した事件に対する解決に中心をおいて運営する専担組識である。可能ならば，予防的な次元でなされるべきであり，他の組織とか機関と同調体制を構築することが，なによりも望ましいと見える。

2）情報倫理の確立の側面からの改善方案に対する考察することができる。情報倫理とは，倫理の問題を情報通信または情報社会の観点で照明したこととして，資料または情報を扱うことにあって，個人とか社会構成員等の行動と規

範体系として，行動と態度を倫理的な観点から判断するようにしてくれる基準である。けれども，情報社会の最も大きい特徴の中の一つが，通信網を通した情報のコミュニケーション化ということである。情報倫理の確立は情報社会を構築するための前提として，そのためには，情報通信倫理に対する明確な価値観の確立が先行にならなければならない。そして，正規教育過程での倫理教育を施行して，コンピュータの実際的な使用と理論的な側面だけを強調する技術教育は止揚しなければならないと考える。このような教育以外にも，新聞とかテレビ等の各種のマスコミが正しい情報倫理の拡散に努力するべきである。

しかし，このような教育方案の提示があっても，個々人の情報社会を生きていく倫理意識の確立が最も重要な部分だとするはずである[81]。

7．おわりに

現代の情報社会には，特に，通信機術の発展によって空間的な距離概念が単一化になって，より迅速な情報の伝達と処理が可能になった。また，発展した情報通信技術は専門家だけではなく情報社会を生きていく人々が共有できる一つの組織とか社会構成的な性格をもっている。このような構成等の土台は通信機術であるが，通信網で流通される情報と財源は，他のどんな社会のそれより大規模的だということである。情報社会の社会問題に現れている特異なことは，その犯罪がコンピュータを利用して犯行をするということである。今まで，情報社会の特徴とした色々な部分の問題点を，コンピューター犯罪の問題，現在の現況，対策等について注意深く考察しました。

結論的にいうと，今からは可能な限りコンピュータ犯罪を防止して改善させて行くことが必要なことだと考えられる。しかし，他のいかなる安全対策とか防止技法が開発されても，一般的で伝統的な犯罪が，どのような社会的な法律とか制度下でも絶えずなされていることと同じに，コンピュータ犯罪もまた，決してなくならないという結果を類推させることができる。結局，各々の自らの倫理意識が情報社会の定着を試みることができることである。

本稿には，逆機能を主にコンピューター犯罪に特別な焦点を合せて分析した。コンピュータをはじめとした情報化技術その自体は，人間の生活の質を高める

のに大きく寄与した文明の利己である。問題は，そういう技術をどのように利用するかにある。情報技術を発展させることも人間で，コンピューター犯罪を起こすこともやはり人間ということである。情報化がコンピューター犯罪を予防できてそれを保護することができる方向で積極的に推進させないと，情報化はその自体が文明の利己でなく，「文明の凶器」になる素地もある。新しい概念の台頭に対する新しい制度，法規，規則などが長期的な観点で設置・制定されないならば，情報社会は私達が予め予見できない程度の混乱を持ってくることになってしまうかもしれない。逆機能が正しく防止することができないと，情報社会は私達が考えることより，一層大きい障害に当面することができるためである。

また，情報社会におけるコンピュータ犯罪に対する専門家がたくさん輩出されて，意識水準を高めてくれるならば，これはコンピュータ犯罪の拡散を防止するのにも大きい影響を与えることと考えられる。

注と参考文献

1）荒木功，「情報化社会論の展開」，早川善次・津金沢聰廣編，『マスコミを学ぶ人のために』，世界思想社，pp.156－157，1987年

2）Bell. Daniel,『the Information Society : Economic Social, and Structual Issues』, Lawrence Earlbaum Associates Publisheres，序論，1989年

3）日立 Digital・平凡社，『世界大百科事典』，1998年

4）小泉修，『デジタル情報化社会の衝撃』，太陽企画出版，p.106，1997年

5）2000年から2010年中葉ぐらい

6）野口宏，『情報社会の理論的探究』，関西大学出版部，p.391，1998年

7）順機能（Eufunction）を正機能ともいう。反対の機能は逆機能（Dysfunction）である。

8）丸山哲夫監訳・編集，『社会学中辞典』，N．アバークロンビー，S．ヒル，B．S．ターナー，『The Penguin Dictionary of Sociology』，ミネルブァ書房，p.103，1996年

9）大前一，『電脳への提言』，アスキー出版局，p.415，1997年

10）福永邦雄，泉 正夫，荻原昭夫，『コンピュータ通信とネットワーク』，共立出版，

p.2, 1998年

11) 田辺孝二,『ネットワーク時代の地球市民の生き方』, 中央経済社, p.222, 1998年

12) 野辺名豊,『崩壊の危機』, アスキー出版局, p.9, 1996年

13) 前川良博,『情報処理と職業倫理』, 日本工業新聞社, p.25, 1989年

14) 金榮建,「情報処理要員の職業倫理意識実態調査比較分析」, 韓国嶺南経営情報学会 論文第2券1号, p.60, 1993. 11月

15) 村上則夫,『高度情報社会と人間』, 松籟社, p.201, 1997年

16) 金鍾範,「情報化社会における逆機能と対策」,『韓国行政研究』, 韓国行政研究院, 1996年

17)『犯罪・非行事典』, 日本大成出版社, pp.153, 1995年

18) 米川茂信,『現代社会病理学』, 学文社, pp.235－236, 1996年

19)『犯罪・非行事典』, pp.264－265, 1995年

20) 朴在春,「コンピュータ犯罪の段階別特性と対応方案に関する研究」, 韓国外国語大学経営情報大学院修士論文, p.13, 1995年

21) 韓国法務部,『コンピュータ犯罪』, p.48, 1984年

22) 朴在春, 前掲書, p.15, 1995年

23) 米川茂信, 前掲書, pp.81－89, 1996年

24)『犯罪・非行事典』, p.139, 1995年

25)『世界大百科事典』, 1998年

26) 金文鎰,『コンピュータ犯罪論』, 法榮社, p.77, 1989年

27) 崔必烈,「情報化時代のコンピュータ犯罪」, 韓国大検察庁, p.4, 1998. 11月, http://www.sppo.go.kr/

28) 板倉宏,「コンピュータ犯罪と刑事法」,『現代社会と新しい刑法理論』, 勁草書房, p.100, 1980年

29) Ulrich Sieber,『The International Handbook on Computer Crime』, John Wiley & Sons, pp.37－92, 1986年

30) 金尹明,「コンピュータ犯罪の問題点と改善方案」, pp.4－5, http://user.chollian.net/~infolaw/crime.htm (韓国)

31) 日本警察庁,『警察白書』, p.15, 1984年

32) Ulrich Sieber，前掲書，p.188，1986年

33) 須藤修，『新しい暗号技術と情報セキュリティへの応用』，東京教育情報センター，p.49，1998年

34) 日本警察庁，http://www.npa.go.jp/

35) 日本警察庁，『日本警察白書』，p.5，1998年

36)『日本警察白書』，前掲書，p.29，1998年

37) 大宮由紀，「コンピュータ犯罪について」，岩手大学，1999. 2月，http://www.hss.iwate-u.ac.jp/~yuki_o/cl/c1teigi.html

38) 1997年，経済協力開発機構（OECD）の国際組織犯罪対策（コンピュータ犯罪捜査体制の強化），コンピュータ犯罪対策についての国際犯罪対策，暗号政策，テロ政策などの様々な観点からサミット，経済協力開発機構（OECD）等を中心に活発な取り組みが進められている。1997年のサミット参加8個国による「P 8国際組織犯罪上級専門家会合」（リヨングループ）にもうけられたコンピュータ犯罪に関するサブグループにおいて協議が進められた。6月に開催されたデンヴァー・サミットで，「国境を越えて介入するようなコンピュータ犯罪者についての捜査，訴追および処罰」と「すべての政府がコンピュータ犯罪に対応する技術的および法的能力を有することとなる体制」について今後1年間得に力を入れて取り組むこととされた。

39) 佐田守弘，「コンピュータ社会と犯罪者」，1998. 4月，http://www4.justnet.ne.jp/~morihiro.sada/pc/secrty01.html

40) 石橋啓一郎訳，『ネットワークセキュリティ』，プレンティスホール出版，p.308，1997年

41) 盧然厚，『コンピュータ犯罪実態と事例の類型』，韓国ハイテク情報，p.63，1992年

42) 紀藤正樹，『電脳犯罪対策虎之巻』，KKベストセラーズ，p.53，1997年

43) ハードウェアなどの有形資産，プログラム・情報などの無形資産を意味する。

44) 三口隆一，「コンピュータ犯罪とその捜査」，1998年，http://www.ceres.dti.ne.jp/

45) Louis Rohner，『Computerkriminalitat』，schulthess polygraphischer，a.a.O，S.4，1976年，

Klaus Tiedemann,『Wirtschaftsstrafrecht und Wiftschaftskriminalitat』, S.150ff, 1976年,

Ulrich Sieber, 前掲書, John Wiley & Sons, pp.37－92, 1986年,

August Bequai,『How to prevent Computer Crime』, 堀部政男・堀田牧太郎 訳編,『情報犯罪』, 啓学出版, p.54, 1986年,

Donn B. Parker,『Computer abuse Assessment』, SRI, pp.29－31, 1975年,『Fighting Computer Crime』, p.15, Charles Scribners Sons, 1983年,

Wolfgang Steinke,『Die Kriminaltat Duruch Beeinflussung von Rechnerablaufen』, Nstz, Heft.S.295, 1984年,

板倉宏,「コンピュータ犯罪と刑法」,『現代社会と新しい刑法理論』, 勁草書房, p.100, 1980年,

門田 渉,「我の国におけるコンピュータ犯罪の現状」, 警察公論, p.21, 1985. 7月,

的場純男,「コンピュータ犯罪に関する刑事法上の問題点」, ジュリスト846号, 有斐閣, 1985. 10月

46) 朴相宅,『コンピュータ犯罪に関する意識調査研究』, 韓国啓明大学修士論文, pp. 6－8, 1993年

47) 小山謙二,『情報セキュリティ』, 電気書院, pp.15－16, 1989年

48) 日本警察庁, http://www.npa.go.jp/

49)『日本警察白書』, 前掲書, p.8, 1998年

50) サイバー空間で行なわれる（地理的・時間的 無制限性）からである。

51) 崔必烈, 前掲書, pp.5－6, 1998. 11月

52)『犯罪・非行事典』, p.254, 1995年

53) 崔必烈, 前掲書, pp.14－15, 1998. 11月

54) オスマー・カヤス, 久保隆之訳,『インターネットセキュリティ』, オーム社, pp. 13－20, 1997年

55) ウィリアム・スターリングス, 森田進訳,『インターネット・セキュリティのすべて』, 日経ＢＰ社, p.35, 1997年

56) 小池澄男,『新・情報社会論』, 学文社, p.150, 1998年

57) 金尹明, 前掲書, pp.6－7

58）日本警察庁，http://www.npa.go.jp/

59）愛知県警，新潟県警

60）広島県警，京都府警

61）福岡県警

62）広島県警，岐阜県警

63）日本警察庁，「警察庁からのお知らせ」，1999. 7. 1日，
http://www.npa.go.jp/police_j.htm

64）Japan Computer Emergency Response Team / Coodrination Center

65）日本コンピュータ緊急対応センター，http://www.jpcert.or.jp/

66）1999年7月1日から1999年9月30日までの動向

67）日本警察庁，「情報セキュリティ・ビジョン策定研究会報告書」，1999. 2月，
http://www.npa.go.jp/police_j.htm

68）日本警察庁にはハイテク犯罪と表現しているが，本稿ではコンピュータ犯罪と明記する。

69）日本警察庁，広報誌「けいさつのまど，121号」，1999年3月

70）日本警察庁，「ハイテク犯罪の検挙状況」，http://www.npa.go.jp/

71）李光享，「インターネットを利用した新種犯罪の実態」，情報化逆機能公聴会，韓国情報保護センター，1999. 9. 8日

72）韓国警察庁，http://www.npa.go.kr/

73）1998. 9. 1日から1998. 9. 30日までの30日間，総1,021件1,681人検挙（拘束364，非拘束1,317）

74）1998. 10. 29日から1998. 12. 31日までの64日間，総35件64人検挙（拘束37，非拘束27）

75）南吉賢，「ハッキング被害および対策」，情報化逆機能公聴会，韓国情報保護センター，1999. 9. 8日

76）申カク撤，金文鎰，『コンピュータ犯罪論』，法英社，pp.194－195，1998年

77）菅野文友，『コンピュータ犯罪のメカニズム』，日科技連，pp.49－52，1990年

78）鳥居壮行，『情報セキュリティ』，オーム社，pp.65－70，1998年

79）設備価値，運営価値，情報価値など

80）道徳性など

81) 社団法人私立大学情報教育協会,『情報倫理概論』, pp.12－13, 1995年

（ほんすんよん　佛教大学大学院社会学研究科博士課程）

Problems and measures of computer crimes

Seung-Yeon, Hong

There happened many changes in various fields, such as the administration, the industry, the finance and the national defense and the medical treatment in the information society. Also, the information society is providing various conveniences with production of a lot of additional values (Eufunction). On the other hand, the dysfunction has appeared to accompany with this, and the range of the accident and the disaster get wide, the damages are increasing by the computer crime.

The computer crime is a new kind of crime in the information society that has appeared as one of such dysfunctions. The more to make information society develops, the more various fields and forms occurs in the computer crime.

If the computer crime can not be controlled, the fact that the developing of information society is something placed in the contradicting situation. It makes us think whether the effort for the study and the control about the computer crime has become more necessary at present.

This paper, in view of the study on the dysfunction which accompanies with the information society and makes the bright and the dark side of the information society, do researches on present situation of the computer crime, with a deep attention to the cases of Japan and Korea.

By offering a plan of the management for the prevention of the computer crime, it tries to improve the study on the computer crime and come up with a measure.